REMARKS

By the foregoing, Claims 1, 11, 18, and 23 have been amended, and claims 19, 21-22, 24-25, and 29-31 have been canceled. Claims 1-18, 20, 23, and 26-28 are pending in the application.

Claim 11 has been amended to address the objections to claim 11 set forth in the Office Action dated July 8, 2005.

The claims have also been amended to clarify the differences between the claimed subject matter and the DeTreville reference (U.S. Patent Publication US 2004/0015694).

In particular, Claim 23 sets forth a method for determining whether a computer has been tampered with by a deceptive interpreter, the method including a computer program receiving a secure attention instruction from a source. Claim 23 further sets forth that if a deceptive interpreter *is not* present, the computer processor retrieves and executes the at least one security check program from the secure memory unit, evaluates the results of the security check program, and transmits the results of the security check program and a cryptographically generated authentication value to the source, but that if a deceptive interpreter *is* present, the computer processor will not retrieve and execute the security check program and will not transmit a correct authentication value to the source. An incorrect or absent authentication value indicates the presence of a deceptive interpreter.

These features are clearly not present in DeTreville. Page 7 of the Office Action discusses some of these features in the paragraph addressing claims 19 and 29, pointing out DeTreville paras [0017]-[0019] and [0078]-[0079]. These paragraphs address curtained code that allows "trusted applications to be executed in a secure manner regardless of the security of the operating system". See para [0037]. Paragraphs [0109 and [0110] describe that access to the curtained code area is limited to certain execution entry points or permits access only through special entry instructions. Paragraph [0114] also describes that the code within the curtained area performs its entire operation "without interruptions from any point outside the secure curtained-memory regions", in order to prevent rogue programs or devices from hijacking the code after its execution has begun. Para [0118] describes the verification of entry points and also describes a determination of whether the instruction seeking access to the curtained code "has the privilege level required to invoke the operation at the desired location".

Nothing in DeTreville describes a method whereby a computer processor executes security check programs retrieved from a secure memory unit after receiving a secure attention instruction, and returns the security check results and an authentication code only if a deceptive interpreter is not present.

Even if the "secure curtained memory regions" or the "curtained code" of DeTreville were considered to correspond to the claimed "secure memory unit", there is no indication that DeTreville's processor uses security check programs retrieved from the curtained code to check

the computer for tampering, and then transmits both the security check results and a correct cryptographically generated authentication code only if a deceptive interpreter is not present.

For at least these reasons, Claim 23 is believed to be allowable over DeTreville.

Independent claims 1, 11, and 18 are believed to be allowable for at least the reasons that Claim 23 is allowable.

The dependent claims are believed to be allowable for at least the reasons that the independent claims are allowable. Nonetheless, a few comments are provided to expedite prosecution.

Claim 28 recites that the the computer processor interrupts execution of other instructions after receipt of the secure attention instruction. The Office Action has not pointed out anything in DeTreville that corresponds to this claimed feature, and it does not appear that DeTreville discloses such a feature.

Claim 17 sets forth that the secure memory unit is accessible via an external connection that bypasses the CPU and all other parts of the secure computer system upon the completion of a cryptographic authentication protocol. The Office Action points to the "curtained code" methodology discussed at paragraph [0037] of DeTreville as corresponding to these features. Applicants note that nothing in DeTreville requires completion of a cryptographic authentication protocol before the curtained code region can be accessed. Indeed, DeTreville at paragraph [0109] and [0110] describe that access to the curtained code area is limited to certain execution entry points or permits access only through special entry instructions such as "curtained-call

instruction, CCAL Ring, Subring, OpIndex". There is no disclosure of a cryptographic authentication protocol.

For at least these additional reasons, claims 28 ans 17 are not anticipated by DeTreville.

Accordingly, the claims are believed to be in condition for allowance. The Examiner is requested to withdraw the anticipation rejections of the pending claims, and to indicate the allowability of the application.

Should there be any questions regarding this Amendment, or the application in general, the examiner is cordially invited to contact the undersigned at the number listed below.

Respectfully submitted,

Date: June 1, 2006

By: Sally Ferrett

Sally A. Ferrett
Registration No. 46,325

Naval Research Laboratory
Office of Associate Counsel (Patents)
4555 Overlook Ave., SW 20375
(202) 404-1551